ABSTRACT

A method for issuing Anonymous Public Key Certificates to Registered Persons in an electronic record system, where pointers for indexing the record system are stored within the Anonymous Public Key Certificates, and where associated Private Keys are controlled by smartcards or similar devices. Electronic records may be identifiably indexed when the smartcard has been activated by its holder correctly entering their secret pass-phrase, or anonymously indexed when only the value of a pointer is known. The only direct linkage between each Anonymous Public Key Certificate and the associated Registered Person is through the associated Private Key as controlled by a smartcard or similar device. Using this invention the retrieval of identifiable records pertaining to a given Registered Person from an electronic record system is normally only possible with the agency of the Person's smartcard or similar device, and therefore normally only possible with the Person's consent.